

HOUSE No. 4012

The Commonwealth of Massachusetts

HOUSE OF REPRESENTATIVES, May 7, 2007.

The committee on Consumer Protection and Professional Licensure to whom was referred the petition (accompanied by bill, Senate, No. 208) of Michael W. Morrissey, Bruce E. Tarr, Denise Provost, Susan C. Tucker and other members of the General Court for legislation relative to security freezes and notification of data breaches, reports recommending that the accompanying bill (House, No. 4012) ought to pass.

For the committee,

MICHAEL J. RODRIGUES.

The Commonwealth of Massachusetts

In the Year Two Thousand and Seven.

AN ACT RELATIVE TO SECURITY FREEZES AND NOTIFICATION OF DATA
BREACHES.

*Be it enacted by the Senate and House of Representatives in General
Court assembled, and by the authority of the same, as follows:*

1 SECTION 1. Chapter 66 of the General laws, as appearing in
2 the 2004 Official Edition, is hereby amended by inserting after
3 section 8A the following new section:—

4 Section 8B. Records or documents shall be destroyed or dis-
5 posed of pursuant to the provisions of chapter 93I of the General
6 laws only in a manner that prevents personal data, as defined in
7 section 1 of chapter 66A, from being practicably read or recon-
8 structed.

1 SECTION 2. Section 1 of chapter 66A of the General Laws, as
2 appearing in the 2004 Official Edition, is hereby amended by
3 striking out the definition “Agency” and inserting in place thereof
4 the following definition:—

5 “Agency”, any county, city, town, judicial branch, constitu-
6 tional office or any agency of the executive branch, including but
7 not limited to, any department, division, bureau, board, commis-
8 sion or committee thereof, or any authority created by the general
9 court to serve a public purpose, having either statewide or local
10 jurisdiction.

1 SECTION 3. Said section 1 of said chapter 66A of the General
2 Laws is hereby amended by striking out the definition “Personal
3 data” and inserting in place thereof the following definition:—

4 “Personal data”, any information concerning a resident of the
5 commonwealth which, because of first name or first initial, and
6 last name, identifying number, or description can be readily asso-
7 ciated with a particular individual, including, but not limited to, a

8 Social Security number, a government-issued driver's license or
9 identification number, or an account number, credit or debit card
10 number, which may or may not be in combination with any
11 required security code, access code, or password that would
12 permit entry to a resident's financial account; provided however,
13 that such information may be redacted, pursuant to paragraph (e)
14 of section 10 of chapter 66, by the custodian or holder of a public
15 record, as defined in clause Twenty-sixth of section 7 of chapter 4
16 prior to the dissemination of any such record; and provided fur-
17 ther, that personal data shall not include intelligence information,
18 evaluative information or criminal offender record information, as
19 defined in section 167 of chapter 6, information available from the
20 sex offender registry, as defined in section 178C of said chapter 6,
21 or information authorized by state or federal law or by an indi-
22 vidual to be publicly listed, published or disseminated or to be
23 transferred to a third party.

1 SECTION 4. Subsection (d) of section 2 of said chapter 66A of
2 the General Laws, as appearing in the 2004 Official Edition, is
3 hereby amended by inserting after the word "fire", the word:—
4 "identity theft"

1 SECTION 5. Section 50 of chapter 93 of the General Laws, as
2 appearing in the 2004 Official Edition, is hereby amended by
3 adding the following definitions:—

4 "Identity theft report," means a report that alleges identity theft
5 pursuant to section 37E of chapter 266, 18 United States Code,
6 section 1028, or a similar statute in any other jurisdiction; or is a
7 copy of an official report filed by a consumer with an appropriate
8 federal, state or local law enforcement agency; and the filing of
9 which subjects the person filing the report to criminal penalties
10 relating to the filing of false information.

11 "Lift" means that the consumer's credit information may be
12 released for a specific party or period of time stated by the con-
13 sumer when there is a security freeze in place.

14 "Password" or "Personal identification number" means a
15 unique and random number or combination of numbers and let-
16 ters, but shall not contain a consumer's social security number or
17 any part of a consumer's social security number, or other personal
18 identifying information.

19 “Proper identification,” means information generally sufficient
20 to identify a person. This does not include information con-
21 cerning the consumer's employment and personal or family his-
22 tory unless the consumer is unable to reasonably identify himself
23 or herself with the information described above.

24 “Security freeze” means a notice placed in a consumer’s credit
25 report at a consumer reporting agency, at the request of the con-
26 sumer and subject to certain exceptions, which prohibits the con-
27 sumer reporting agency from releasing the consumer’s report or
28 any information from it without the express authorization of the
29 consumer.

1 SECTION 6. Clause (b) of section 56 of chapter 93 of the
2 General Laws, as so appearing, is hereby amended by adding the
3 following paragraphs at the end thereof:—

4 “You have a right to request a “security freeze” on your credit
5 report. The security freeze will prohibit a consumer reporting
6 agency from releasing any information in your consumer report
7 (also known as your credit report) without your express authoriza-
8 tion. A security freeze must be requested by sending a written
9 request via certified mail, overnight mail, or regular stamped mail
10 to a consumer reporting agency. The security freeze is designed to
11 prevent credit, loans, and services from being approved in your
12 name without your consent. You should be aware that using a
13 security freeze may delay, interfere with, or prevent the timely
14 approval of any subsequent request or application you make
15 regarding new loans, credit, mortgage, insurance, government
16 services or payments, rental housing, employment, investment,
17 license, cellular phone, utilities, digital signature, internet credit
18 card transaction, or other services, including an extension of credit
19 at point of sale.

20 “When you place a security freeze on your credit report, within
21 5 business days of your request for a security freeze the consumer
22 reporting agency will provide you with a personal identification
23 number or password to use if you choose to remove the freeze on
24 your credit report or authorize the release of your credit report for
25 a specific party, parties or period of time after the freeze is in
26 place. To provide that authorization, you must contact the con-
27 sumer reporting agency and provide all of the following:

28 (1) the personal identification number or password provided by
29 the credit reporting agency;

30 (2) proper identification to verify your identity; and

31 (3) the proper information regarding the third party or parties
32 who are to receive the credit report or the period of time for which
33 the report shall be available to users of the credit report.

34 "A consumer reporting agency that receives a request from a
35 consumer to temporarily lift a freeze on a credit report shall
36 comply with the request no later than 3 business days after
37 receiving the request.

38 "A security freeze does not apply to a person or entity, or to its
39 affiliates, or collection agencies acting on behalf of the person or
40 entity, with which you have an existing account that requests
41 information in your credit report for the purposes of reviewing or
42 collecting the account, provided you have previously given your
43 consent to use of your credit reports. Reviewing the account
44 includes activities related to account maintenance, monitoring,
45 credit line increases, and account upgrades and enhancements."

1 SECTION 7. Section 55 of said chapter 93, as so appearing, is
2 hereby amended by inserting after the word "fifty-one" the
3 following words:— and section sixty-two-A

1 SECTION 8. Chapter 93 of the General Laws, as so appearing,
2 is hereby amended by inserting after section 62 the following
3 section:—

4 Section 62A. Security Freeze on Consumer Report:—

5 If a consumer requests a security freeze, the consumer reporting
6 agency shall disclose to the consumer the process of placing,
7 removing and lifting a security freeze. A consumer reporting
8 agency shall require proper identification of the person making a
9 request to place, lift or remove a security freeze.

10 A consumer may request that a security freeze be placed on his
11 or her consumer report by sending a request in writing via certi-
12 fied mail, overnight mail, or regular stamped mail to a consumer
13 reporting agency at an address designated by the consumer
14 reporting agency to receive such requests. If a security freeze is in
15 place, the information from a consumer's report may not be
16 released to a third party without prior express authorization from

17 the consumer. This section does not prevent a consumer reporting
18 agency from advising a third party that a security freeze is in
19 effect with respect to the consumer's report.

20 A consumer reporting agency shall place a security freeze on a
21 consumer's report no later than 3 business days after receiving a
22 written request from the consumer. The consumer reporting
23 agency shall send a written confirmation of the security freeze to
24 the consumer within 5 business days after receiving the written
25 request and shall provide the consumer with a unique personal
26 identification number or a unique password or both to be used by
27 the consumer when providing authorization for the removal or
28 lifting of the security freeze.

29 If the consumer wishes to lift a security freeze that is in place,
30 he or she shall contact the consumer reporting agency, request that
31 the freeze be lifted, and provide proper identification, the personal
32 identification number or password or both, provided by the con-
33 sumer reporting agency, and proper information regarding the
34 third party who is to receive the consumer report or the time
35 period for which the report shall be available to users of the con-
36 sumer report.

37 A consumer reporting agency that receives a request from a
38 consumer to lift a security freeze on a consumer report pursuant to
39 this chapter shall comply with the request no later than 3 business
40 days after receiving the request.

41 A consumer reporting agency may develop procedures
42 involving the use of telephone, fax, the Internet, or other elec-
43 tronic media to receive and process a request from a consumer to
44 lift a security freeze or remove a security freeze on a consumer
45 report in an expedited manner.

46 A security freeze shall remain in place until the consumer
47 requests that the security freeze be lifted or removed in the
48 manner provided in this section; provided, however, that a con-
49 sumer reporting agency may remove a security freeze if the con-
50 sumer's report was frozen due to a material misrepresentation of
51 fact by the consumer. If a consumer reporting agency intends to
52 remove a freeze upon a consumer's report due to a material mis-
53 representation of fact by the consumer, the consumer reporting
54 agency shall notify the consumer in writing 5 business days prior
55 to removing the freeze on the consumer's report.

56 When a security freeze is in place, a consumer reporting agency
57 shall not change any of the following official information in a
58 consumer report without sending a written confirmation of the
59 change to the consumer within 30 days of the change being posted
60 to the consumer's file: name, date of birth, social security number,
61 and address. Written confirmation is not required for technical
62 modifications of a consumer's official information, including
63 name and street abbreviations, complete spellings, or transposition
64 of numbers or letters. In the case of an address change, the
65 written confirmation shall be sent to both the new address and to
66 the former address.

67 If a third party requests access to a consumer report on which a
68 security freeze is in effect, and this request is in connection with
69 an application for credit or any other use, and the consumer does
70 not allow his or her credit report to be accessed for that specific
71 party or period of time, the third party may treat the application as
72 incomplete.

73 A consumer reporting agency shall remove a security freeze
74 within 3 business days of receiving a request for removal from a
75 consumer who provides both proper identification and the per-
76 sonal identification number or password provided by the con-
77 sumer reporting agency pursuant to this chapter.

78 The provisions of this chapter do not apply to the use of a con-
79 sumer report by any of the following:

80 1) a person or entity, or a subsidiary, affiliate, or agent of that
81 person or entity, or an assignee of a financial obligation owing by
82 the consumer to that person or entity, or a prospective assignee of
83 a financial obligation owing by the consumer to that person or
84 entity in conjunction with the proposed purchase of the financial
85 obligation, with which the consumer has or had prior to assign-
86 ment an account or contract, including a demand deposit account,
87 or to whom the consumer issued a negotiable instrument, for the
88 purposes of reviewing the account or collecting the financial
89 obligation owing for the account, contract, or negotiable instru-
90 ment. For purposes of this paragraph, "reviewing the account"
91 includes activities related to account maintenance, monitoring,
92 credit line increases, and account upgrades and enhancements; a
93 subsidiary, affiliate, agent, assignee, or prospective assignee of a
94 person to whom access has been granted under for purposes of
95 facilitating the extension of credit or other permissible use;

96 2) any federal, state or local agency, law enforcement agency,
97 trial court, or acting pursuant to a court order, warrant, or sub-
98 poena;

99 3) the Massachusetts child support agency under Title IV-D of
100 the Social Security Act (42 U.S.C. et seq.);

101 4) the executive office of health and human services or its
102 agents or assigns acting to investigate Medicaid fraud;

103 5) the department of revenue or its agents or assigns acting to
104 investigate or collect delinquent taxes or unpaid court orders or to
105 fulfill any of its other statutory responsibilities;

106 6) a person or entity using credit information for the purposes
107 of prescreening as provided for by the federal Fair Credit
108 Reporting Act;

109 7) any person or entity administering a credit file monitoring
110 subscription service to which the consumer has subscribed;

111 8) any person or entity acting solely for the purpose of pro-
112 viding a consumer with a copy of his or her credit report upon the
113 consumer's request; or

114 This section does not prevent a consumer reporting agency
115 from charging a reasonable fee not to exceed 10 dollars to a con-
116 sumer who requests to place a security freeze, except that a con-
117 sumer reporting agency shall not charge a fee to a victim of
118 identity theft who provides an identify theft report to the con-
119 sumer reporting agency, provided that the identity theft report is
120 accompanied by a police report filed in response to the identity
121 theft in the appropriate municipality.

122 This section does not prevent a consumer reporting agency
123 from charging a reasonable fee not to exceed 10 dollars to a con-
124 sumer who elects to lift the security freeze. No fee shall be
125 charged for a permanent removal of a security freeze.

126 The following entities or persons are not required to place a
127 security freeze on a consumer report:

128 1) a check services or fraud prevention services company,
129 which issues reports on incidents of fraud or authorizations for the
130 purpose of approving or processing negotiable instruments, elec-
131 tronic funds transfers, or similar methods of payments;

132 2) a deposit account information service company, which issues
133 reports regarding account closures due to fraud, substantial over-
134 drafts, ATM abuse, or similar negative information regarding a

135 consumer, to inquiring banks or other financial institutions for use
136 only in reviewing a consumer request for a demand deposit
137 account at the inquiring bank; or

138 3) a consumer reporting agency that acts only as a reseller of
139 credit information by assembling and merging information con-
140 tained in the database of another consumer reporting agency or
141 multiple consumer credit reporting agencies, and does not main-
142 tain a permanent database of credit information from which new
143 consumer credit reports are produced; provided, however, that
144 such financial institution or consumer reporting agency shall be
145 subject to any security freeze placed on a consumer report by
146 another consumer reporting agency from which it obtains informa-
147 tion.

1 SECTION 9. Section 63 of said chapter 93, as so appearing, is
2 hereby amended by striking out the words “sixty-two” and
3 inserting in place thereof the following word:— sixty-two-A

1 SECTION 10. Section 64 of said chapter 93, as so appearing,
2 is hereby amended by striking out the word “sixty-two”, in the
3 first sentence, and inserting in place thereof the following word:—
4 sixty-two-A

1 SECTION 11. The General Laws, as so appearing, is hereby
2 amended by inserting after Chapter 93G the following new
3 chapter:—

4 **Chapter 93H: Security Breaches**

5 Section 1. The following words as used in this chapter shall,
6 unless the context clearly requires otherwise, have the following
7 meanings:

8 “Agency” means any agency, executive office, department,
9 board, commission, bureau, division or authority of the common-
10 wealth, or any of its branches, or of any political subdivision
11 thereof.

12 “Breach of the security of the system” means the unauthorized
13 acquisition of data that may compromise the security, confiden-
14 tiality, or integrity of personal information maintained by a com-

15 mercial entity or agency. Good faith but unauthorized acquisition
16 of personal information by an employee or agent of a commercial
17 entity or agency for the purposes of the commercial entity or
18 agency is not a breach of the security of the system, provided that
19 the personal information is not used in an unauthorized manner or
20 subject to further unauthorized disclosure.

21 “Commercial entity” means an individual, corporation, busi-
22 ness trust, estate, trust, partnership, limited partnership, limited
23 liability partnership, company, limited liability company, associa-
24 tion, organization, joint venture or any other legal, whether for
25 profit or not-for-profit, conducting business or operating in
26 Massachusetts, but does not mean an agency as defined in this
27 chapter.

28 “Notice” means

29 (i) written notice;

30 (ii) electronic notice, if the notice provided is consistent with
31 the provisions regarding electronic records and signatures set
32 forth in § 7001 (c) of Title 15 of the United States Code; and
33 section 110G of the General Laws; or

34 (iii) substitute notice, if the commercial entity or agency
35 required to provide notice demonstrates that the cost of providing
36 written notice will exceed \$250,000, or that the affected class of
37 Massachusetts residents to be notified exceeds 500,000 residents,
38 or that the commercial entity or agency does not have sufficient
39 contact information to provide notice.

40 “Substitute notice” consists of all of the following:

41 (i) electronic mail notice if the commercial entity or agency
42 has electronic mail addresses for the members of the affected class
43 of Massachusetts residents; and

44 (ii) clear and conspicuous posting of the notice on the home
45 page of the Web site of the commercial entity or agency if the
46 commercial entity or agency maintains a web site; and

47 (iii) notice to major statewide media.

48 “Personal information” means a Massachusetts resident’s first
49 name and last name or first initial and last name in combination
50 with any 1 or more of the following data elements that relate to
51 the resident:

52 a. Social Security number;

53 b. Driver’s license number or state-issued identification card
54 number;

55 c. or Financial account number, or credit or debit card number,
56 if unauthorized use of said account does not require a security
57 code, access code, or password to be accessed or used.

58 Section 2. The executive office of consumer affairs and busi-
59 ness regulations shall establish regulations for commercial entities
60 that own or license from another personal information about a res-
61 ident of Massachusetts, and the regulations shall be designed to
62 safeguard the personal information of Massachusetts residents.
63 The objectives of the regulations shall be to insure the security
64 and confidentiality of customer information; protect against antic-
65 ipated threats or hazards to the security or integrity of such infor-
66 mation; and protect against unauthorized access to or use of such
67 information that could result in substantial harm or inconvenience
68 to any customer. The regulations shall take into account the com-
69 mercial entities' sizes, scopes and types of businesses, the amount
70 of available resources to the commercial entities, the amount of
71 stored data, and the need for security and confidentiality of both
72 customer and employee information.

73 The division of public records shall establish rules and regula-
74 tions for agencies that owns or licenses from another personal
75 information about a resident of Massachusetts and shall take into
76 account the agencies' sizes, scopes and types of services the
77 agency provides, the amount of available resources to the agency,
78 the amount of stored data, and the need for security and confiden-
79 tiality of both customer and employee information.

80 Section 3. A commercial entity that owns or licenses from
81 another data that includes personal information about a resident of
82 Massachusetts shall give notice to a resident of Massachusetts of
83 any breach of the security of the system in which the data is held
84 as soon as possible following the discovery of a breach in the
85 security of the system such that the personal information of the
86 Massachusetts resident was, or should reasonably be believed to
87 have been, acquired by an unauthorized person or used for an
88 unauthorized purpose.

89 A commercial entity or agency that maintains or stores but does
90 not own or license from another data medium that includes per-
91 sonal information shall give notice to and cooperate with the
92 owner or licensor of the information of any breach of the security
93 of the system as soon as possible following discovery of a breach,

94 if the said data is reasonably be believed to have been acquired by
95 an unauthorized person or used for an unauthorized purpose.

96 Section 4. An agency that maintains data that includes personal
97 information about a resident of Massachusetts shall give notice to
98 a resident of Massachusetts of any breach of the security of the
99 system as soon as possible following the discovery of a breach in
100 the security of system such that the personal information of the
101 Massachusetts resident was, or should reasonably be believed to
102 have been, acquired by an unauthorized person or used in an
103 unauthorized manner.

104 Section 5. Notice required by this chapter may be delayed if a
105 law enforcement agency determines and informs the commercial
106 entity or agency that the notice will impede a criminal investiga-
107 tion. Notice delayed pursuant to this section must be made in
108 good faith, without unreasonable delay and as soon as possible
109 after the law enforcement agency determines and informs the
110 commercial entity or agency that notification will no longer
111 impede the investigation. The commercial entity or agency shall
112 cooperate with law enforcement on investigating a breach, which
113 includes the sharing of information about an owner or licensee
114 information relevant to the breach; provided however, that such
115 disclosure shall not require the disclosure of confidential business
116 information or trade secrets.

117 Section 6. A commercial entity or agency that is required to
118 give notice of a breach in the security of a system pursuant to this
119 chapter shall also provide written notification of the nature and
120 circumstances of the breach to the attorney general and the state
121 regulatory agency that regulates the commercial entity, if any, as
122 soon as possible following the discovery of a breach in the secu-
123 rity of system. In addition, if such agency is within the executive
124 department, it shall provide written notification of the nature and
125 circumstances of the breach to the information technology divi-
126 sion and the division of public records as soon as possible
127 following the discovery of a breach in the security of system, and
128 shall comply with all policies and procedures adopted by that divi-
129 sion pertaining to the reporting and investigation of breaches of
130 the system.

131 Section 7. This chapter does not relieve a commercial entity or
132 agency from the duty to comply with requirements of any applic-

133 able general or special law or federal law regarding the protection
134 and privacy of personal information; provided however, a com-
135 mercial entity that is regulated by federal law and that maintains
136 procedures for a breach of the security of the system pursuant to
137 the laws, rules, regulations, guidance, or guidelines established by
138 its primary or functional federal regulator is deemed to be in com-
139 pliance with this chapter if the commercial entity notifies affected
140 Massachusetts residents in accordance with the maintained and
141 required procedures when a breach occurs; provided further that
142 the commercial entity also notifies the Attorney General of the
143 breach within three days of its occurrence. Notification to the
144 Attorney General shall consist of, but not be limited to, the steps
145 the commercial entity has taken or plans to take relating to the
146 breach pursuant to the applicable federal regulation or statute;
147 provided further that if said entity does not comply with federal
148 laws, rules and regulations pursuant to its regulator then it shall be
149 subject to the provisions of this chapter.

150 Section 8. The attorney general may bring an action pursuant
151 to section 4 of chapter 93A against a commercial entity or other-
152 wise to remedy violations of this chapter, and for other relief that
153 may be appropriate.

1 SECTION 12. The General Laws, as so appearing, is hereby
2 amended by inserting after Chapter 93H the following new
3 chapter:—

4 **Chapter 93I: Disposition and Destruction of Records.**

5 Section 1. The following word as used in this chapter shall,
6 unless the context clearly requires otherwise, have the following
7 meanings:

8 “Data subject”, an individual to whom personal information, as
9 defined in section 1 of chapter 93H of the General laws, refers.

10 Section 2. When disposing of records, each agency or commer-
11 cial entity shall meet the following minimum standards for proper
12 disposal of records containing personal information:—

13 (a) Paper documents containing personal information shall be
14 either redacted, burned, pulverized or shredded so that personal
15 data cannot practicably be read or reconstructed;

16 (b) Electronic media and other non-paper media containing per-
17 sonal information shall be destroyed or erased so that personal
18 information cannot practicably be read or reconstructed.

19 Each agency or commercial entity disposing of personal infor-
20 mation, after due diligence, may contract with a third party to dis-
21 pose of personal information in accordance with this chapter. Any
22 third party explicitly hired to dispose of material containing per-
23 sonal information shall implement and monitor compliance with
24 policies and procedures that protect against unauthorized access to
25 or acquisition of or use of personal information during the collec-
26 tion, transportation and disposal of personal information.

27 Whoever violates this section shall be subject to a civil fine of
28 \$100 per data subject affected, but not to exceed \$50,000 for each
29 improper disposal; provided, however, that the fine shall not pre-
30 clude a private right of action to recover actual damages.

31 Section 3. The attorney general shall have the sole authority to
32 seek enforcement of this section under the provisions of
33 Chapter 93A.

1 SECTION 13. Chapter 266 of the General Laws, as appearing
2 in the Official Edition of 2004, is hereby amended by inserting
3 after paragraph (e) of section 37e the following paragraph:—

4 (f) A law enforcement officer shall accept a police incident
5 report from a victim and shall return a copy, if requested, within
6 24 hours.

1 SECTION 14. This act shall take effect upon passage.